CRM-ES
CONSELHO REGIONAL DE MEDICINA DO ESTADO DO ESPÍRITO SANTO

Política de Segurança da Informação
do CRM - ES

SUMÁRIO

Política de Segurança da Informação - CRM-ES ..... Erro! Indicador não definido.
1. Introdução **3**
2. Normas de Segurança da Informação e do uso da infraestrutura de rede **4**
2.1 Compete ao setor de Tecnologia da Informação **4**
3. Normas de uso de chaves de acesso para usuários **4**
3.1 Identificação **4**
3.2 Concessão da chave de acesso **5**
3.3 Formação de contas e senhas **5**
3.4 Tempo de vida de contas e senhas **5**
3.5 Disposições Gerais **6**
4. Normas e Diretrizes quanto ao uso da internet **6**
4.1 Orientações **9**
4.2 Realização de Downloads **10**
4.3 Execução de jogos e rádios on-line ou outros serviços de streaming **10**
4.4 Senhas de acesso **10**
5. Utilização do Correio Eletrônico (E-mail) **11**
5.1 Regras para criação de e-mails e listas de discussão de e-mails **12**
6. Normas para Armazenamento de Arquivos **13**
7. Direitos e deveres dos usuários **14**
8. Disposições Finais **15**
9. Penalidades **16**
10. Membros Responsáveis **17**
11. Vigência e Validade **17**
12. Legislação **17**
13. ANEXO I - Termo Individual de Responsabilidade **19**
14. Glossário **20**
15. Histórico de Revisores **21**

1. Introdução

Com o aumento do uso de sistemas conectados que dependem da internet e nuvem de dados, surgem preocupações diretamente ligadas aos dados ou informações de uma instituição. Assim, com o avanço dessa ferramenta e suas diversas formas de utilização, faz-se necessária uma Política que defina as diretrizes para a Segurança da Informação, que vise garantir a integridade, confidencialidade e disponibilidade das informações sob responsabilidade dessa instituição. Uma Política de Segurança descreve a conduta adequada para o manuseio, controle e proteção das informações, contra destruição, modificação, divulgação indevida e acessos não autorizados, seja acidental ou intencionalmente.

Esta Política se aplica às informações sob responsabilidade do Conselho Regional de Medicina do Estado do Espírito Santo – CRM-ES, em qualquer forma ou meio que a informação seja apresentada ou compartilhada, que deverão estar sempre protegidas adequadamente, de acordo com controles definidos nesta política.

Estas normas devem ser divulgadas para todos os empregados da instituição e obedecidas por todos que utilizam os recursos de arquivamento, de disponibilidade e de consultas às informações disponibilizadas e armazenadas pelo setor de Tecnologia da Informação, sendo de responsabilidade de cada um o seu cumprimento. A Política está disponível em formato digital e acessível a todos os empregados da instituição nos meios de comunicação internos.

O cumprimento das normas presentes nesta Política de Segurança será acompanhado e auditado pelo setor de Tecnologia da Informação do CRM-ES. A instituição, mediante autorização expressa da alta direção, se reserva o direito de monitorar, automaticamente, a estação de trabalho, o tráfego efetuado através das redes de comunicação, incluindo o acesso à internet e o uso do correio eletrônico (e-mail).

A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas.

Este documento será revisado periodicamente, ou a qualquer momento em caso de necessidades de atualizações de segurança a critério do setor de Tecnologia da Informação.

2. Normas de Segurança da Informação e do uso da infraestrutura de rede

A segurança é um dos assuntos mais importantes dentre as preocupações de qualquer entidade: confidencialidade, integridade e disponibilidade da informação estão diretamente ligadas à segurança.

A Segurança da Informação é composta de mecanismos que promovem a integridade de uma estrutura de rede na qual trafegam informações e dados comuns e/ou restritos, incluídos os equipamentos que armazenam tais informações. Possibilitando tornar estas informações confiáveis e garantindo que o seu uso não trará nenhuma consequência danosa tanto para o próprio usuário como para a instituição e outros empregados.

A utilização das redes de dados corporativas do CRM-ES não deverá ser utilizada para conexão de dispositivos pessoais dos empregados ou de terceiros.

2.1 Compete ao setor de Tecnologia da Informação

O setor de Tecnologia da Informação tem atribuição para atuar sobre os equipamentos deste Conselho:

Com prévio aviso e autorização da Diretoria, o que concerne aos seguintes tópicos:

a) Realização de auditoria (local ou remota);

b) A instalação de softwares de monitoramento;

Com autonomia, o que concerne aos seguintes tópicos:

c) A definição de perfis de usuários cujos privilégios não permitam a realização de atividades tidas como nocivas ao sistema operacional ou à rede como um todo;

d) A desinstalação de quaisquer softwares instalados sem autorização expressa ou considerados nocivos à integridade da infraestrutura;

e) O credenciamento/descredenciamento de usuários;

3. Normas de uso de chaves de acesso para usuários

Esta norma tem como objetivo estabelecer os procedimentos adequados para a correta utilização das chaves de acesso no ambiente de Tecnologia da Informação do CRM-ES.

Esta norma deverá ser aplicada a todos os empregados que possuam chave de acesso (sem privilégios de “administrador”) nos ativos do tipo estações de trabalho e servidores do ambiente de tecnologia da Informação do CRM-ES. Entende-se como chave de acesso a união de um nome de usuário e uma senha.

3.1 Identificação

A identificação do empregado por senha ou qualquer outro meio é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas através dela, sendo pré-requisito para a liberação do uso o preenchimento de um termo de responsabilidade, indicando as suas condições de uso, seus direitos e deveres.

3.2 Concessão da chave de acesso

a) Para a definição do nome de usuário é adotada a seguinte nomenclatura: iniciais dos nomes + o sobrenome. Ex.: Nome: Maria Ferreira Cardoso = Usuário: mfcardoso.
b) Solicitações de mudanças nos sistemas liberados e/ou permissões para o caso de empregados que já possuam chave de acesso, deverão partir do seu Superior Hierárquico seguindo o mesmo fluxo descrito no item “b”. O setor de Tecnologia da Informação irá submeter a solicitação à aprovação da Gerência para prosseguir com o atendimento.

3.3 Formação de contas e senhas

a) As senhas para usuários deverão conter no mínimo 08 (oito) caracteres, sendo obrigatório o uso de números, letras maiúsculas, minúsculas e caracteres especiais ($, %, &, *, #).
b) Deverá ser evitada a composição de senhas com somente sequências numéricas (123...) e/ou alfabéticas (abc...), além de senhas de fácil dedução (nome da máquina, nome/sobrenome do usuário, data de nascimento e outros).

3.4 Tempo de vida de contas e senhas

Quando possível, as seguintes restrições serão impostas:

a) O usuário deverá ser forçado a trocar a senha no seu primeiro acesso;
b) O tempo mínimo, por vontade do usuário, para troca de senhas deverá ser de dois dias;
c) A conta deverá ser bloqueada após a terceira tentativa sem sucesso de login;
d) O tempo de vida das senhas será de prazo limitado a critério do setor de Tecnologia da Informação, quando deverá ser forçada a sua troca no primeiro login após esse período;

e) Contas que ficarem inativas por mais de 60 dias poderão ser bloqueadas.

3.5 Disposições Gerais

a) A chave de acesso é pessoal e intransferível, devendo ser mantida em sigilo. O usuário será responsabilizado pelo mau uso da chave de acesso;

b) Os sistemas e aplicações deverão ter algum mecanismo que impeça a exibição na tela da senha do usuário;

c) Os sistemas e aplicações deverão ter algum mecanismo que impeça a mesma conta de estar ativa, simultaneamente, em mais de uma estação;

d) O setor de Recursos Humanos deverá comunicar ao Setor de Tecnologia da Informação acerca dos empregados que forem desligados do CRM-ES, para que a chave de acesso seja cancelada e a conta de e-mail encerrada;

e) Deve-se atribuir às contas de usuário somente os privilégios necessários à execução de sua atividade;

f) Os usuários não terão contas com perfil administrador, nem contas do domínio com privilégio de administrador local da estação, exceto para aqueles cuja atividade funcional necessite de tal requisito. Caso necessário, deverá ser solicitado pela chefia do setor com uma justificativa, que será avaliada pela Gerência e pelo setor de Tecnologia da Informação.

g) Os acessos e as falhas nas tentativas de acesso deverão ser auditáveis;

h) A eventual necessidade de instalação de softwares deve ser submetida por abertura de chamado no sistema de help desk ou por e-mail, ao Setor de Tecnologia da Informação, para que haja um controle centralizado de softwares e licenças disponíveis para o Órgão.

i) O empregado é pessoalmente responsável por todas as atividades realizadas por intermédio de sua chave de acesso.

4. Normas e Diretrizes quanto ao uso da internet

Considerando que o uso da Internet é fundamental para as atividades desenvolvidas no CRM-ES e observando-a como ferramenta que possibilita crescentes ameaças às informações da Instituição é de extrema importância que se estabeleça um conjunto de regras que possibilitem a utilização adequada desse importante recurso tecnológico.

Estas normas e diretrizes têm como objetivo estabelecer responsabilidades e requisitos

básicos de utilização da internet nos setores do CRM-ES.

A internet deve ser utilizada para fins de complemento às atividades do setor, para o enriquecimento intelectual de seus empregados ou, no caso dos técnicos em Tecnologia da Informação, como ferramenta para busca por informações que venham contribuir para o desenvolvimento de seus trabalhos.

Com base nos procedimentos de proteção e integridade dos sistemas de informação, a internet é classificada como conexão de alto risco. Os empregados devem estar cientes da periculosidade da navegação na internet, antes de acessá-la e de utilizar os seus recursos.

Todos os empregados que utilizam os recursos tecnológicos de propriedade ou controlados pelo CRM-ES, deverão exercer tal direito de utilização no estrito interesse do órgão, mantendo uma conduta profissional, especialmente em se tratando da utilização de bem público.

O uso recreativo da Internet WIFI de funcionário é liberado para os dispositivos móveis pessoais nos horários de descanso, sendo vedadas quaisquer ações e utilização de serviços que infrinjam legislações vigentes ou que desrespeitem os direitos dos empregados. O CRM-ES não se responsabiliza por eventuais danos ou prejuízos decorrentes do uso deste serviço. O CRM-ES resguarda o direito de suspender o serviço a qualquer momento a seu critério.

Qualquer usuário a quem se tenha dado o direito de se conectar à rede deve fazê-lo para uso exclusivo em serviço.

a) O CRM-ES possui mecanismos de autenticação, que determinam a titularidade de todos os acessos à internet feito por seus empregados.
b) É expressamente proibida a divulgação e/ou compartilhamento indevido de informações sigilosas em listas de discussão ou bate-papo, sejam internas ou externas.
c) A infraestrutura CRM-ES e os recursos de informática jamais devem ser utilizados para a realização de trabalhos de terceiros ou de atividades paralelas.
d) O acesso à internet por parte dos empregados usuários da rede de computadores do CRM-ES deve ser feito exclusivamente por meio da única ligação existente entre a internet e o Conselho. É vedado o acesso à internet utilizando provedores de acesso privados, bem como conexões móveis como 3G e 4G para o acesso à rede mundial de computadores.
e) A privacidade no acesso à internet e ao uso do correio eletrônico é garantida, mas os endereços acessados serão registrados e o conteúdo das informações trafegadas por meio eletrônico poderá ser rastreado, registrado e /ou eliminado de forma automática, por softwares especiais, em busca de termos ou assuntos que

se insiram no grupo de temas cujo acesso ou tráfego é proibido.

f) É vedado o acesso aos sites da internet com conteúdo pornográfico ou ofensivo aos direitos humanos.

g) Todos os acessos à internet serão passíveis de monitoração e identificação, sendo tais acessos arquivados e mantidos disponíveis para cálculos estatísticos, bem como eventuais auditorias.

h) Relatórios gerenciais dos sites acessados por empregados num determinado período poderão ser gerados a critério do Setor de Tecnologia da Informação. A Diretoria poderá ter acesso a essas informações a qualquer tempo.

i) É vedada invasão de computadores alheios para obtenção de senhas e informações pessoais;

j) É vedada a utilização da banda de internet para baixar músicas tipo MP3 ou ouvir rádios on-line;

k) É proibido fazer download de qualquer arquivo ou programa que não sejam de domínio público ou que não sejam apropriados para uso em serviço.

l) O empregado será responsável pelo uso dos serviços providos pelo CRM-ES para acesso à internet, em observância a todas as leis, decretos e regulamentos nacionais, estaduais, e municipais aplicáveis de acordo com estas normas, bem como com a ordem pública.

m) O empregado não poderá transmitir, difundir ou disponibilizar a terceiros informações, dados, conteúdos, mensagens, gráficos, desenhos, arquivos de som e/ou imagens, fotografias, gravações, software e, em geral qualquer classe de material que:

    i. De qualquer forma contrariem, menosprezem ou atentem contra os direitos fundamentais e as liberdades públicas reconhecidas constitucionalmente, nos tratados internacionais e no ordenamento jurídico como um todo;
    ii. Induzam, incitem ou promovam atos ilegais, denegridores, difamatórios, infames, violentos, terroristas ou, em geral contrários à lei;
    iii. Transgridam os segredos empresariais de terceiros;
    iv. Constituam publicidade de qualquer natureza ou conteúdo;
    v. Incorporem vírus ou outros elementos físicos ou eletrônicos que possam causar danos ou impedir o normal funcionamento da rede, do sistema ou de equipamentos informáticos (hardware e software) do CRM-ES ou de

terceiros, ou que possam causar dano aos documentos eletrônicos e arquivos armazenados nestes equipamentos informáticos;

vi. Provoquem, por suas características (tais como forma, extensão, etc.) dificuldades no normal funcionamento da rede local do CRM-ES, bem como da internet;

n) Não é permitido o uso de software de comunicação instantânea, tais como, Facebook Messenger, Whatsapp ou de qualquer outro mecanismo que venha promover serviço semelhante. Exceto com permissão do seu Superior Hierárquico, Gerência Administrativa e Diretoria do CRM-ES como ferramenta de apoio ao trabalho.

o) Não é permitida a utilização de software do tipo *peer-to-peer* (P2P), tais como, Emule, µtorrent e afins.

p) As redes sociais são ferramentas de comunicação e compartilhamento de conhecimentos semelhantes a e-mail e sites, portanto, devem atender as mesmas políticas de uso, ou seja, somente devem ser utilizadas com finalidades de interesse do CRM-ES.

q) É de responsabilidade de cada empregado zelar pelo fiel cumprimento ao estabelecido na presente norma.

r) A não observância de qualquer item acima implicará nas sanções previstas nos Atos Normativos do Plano de Cargos, Carreira e Salários do CRM-ES aprovado pela Resolução CRM-ES n.º 338/2025.

s) Qualquer violação dessas normas cometida pelo empregado ou por terceiro utilizando-se de sua senha pessoal será de responsabilidade do empregado, implicando na adoção das medidas legais aplicáveis, eximindo-se o CRM-ES de qualquer responsabilidade advinda de tal infração.

t) O empregado é pessoalmente responsável por todas as atividades realizadas por intermédio de sua chave de acesso, salvo se comprovadamente tenha havido quebra da sua senha de segurança.

4.1. Orientações

O esquema de bloqueio de sites é baseado em sistemas automatizados, pode ocorrer de algumas páginas serem bloqueadas indevidamente. Caso seja bloqueado um site cujo conteúdo esteja de acordo com esta norma, o empregado pode solicitar o desbloqueio através

da abertura de um chamado no sistema de helpdesk ou enviando um e-mail para helpdesk@crmes.org.br, com uma captura da tela de que foi bloqueada.

4.2 Realização de Downloads

O processo de realização de *downloads* exige boa parte da banda de navegação disponível e, quando realizado em demasia, congestiona o tráfego, compromete sistemas que funcionam on-line além de prejudicar a velocidade de navegação dos demais empregados.

Como o Conselho possui sistemas que realizam constantemente *downloads* de atualizações dos softwares, a tarefa de *downloads* deve ser vista com muito cuidado e sua realização feita somente em casos de extrema necessidade.

Portanto, o empregado que utilizar-se da infraestrutura do CRM-ES para efetuar downloads de arquivos pessoais terá seu tráfego monitorado e encaminhado a chefias e, se necessário, à Diretoria.

4.3 Execução de jogos e rádios on-line ou outros serviços de streaming

Uma vez que não existem quaisquer pertinências com as finalidades institucionais propostas pelo CRM-ES, é terminantemente proibida a execução de serviços de streaming como jogos, músicas, vídeos ou rádios on-line, visto que esta prática toma parte da banda de navegação de internet, dificultando a execução de outros serviços do CRM-ES que necessitam deste recurso. Entretanto, caso seja necessária a liberação de alguns serviços específicos de vídeo ou rádio, por necessidade de serviço, o Superior Hierárquico deverá realizar a abertura de chamado no sistema de helpdesk ou via e-mail para helpdesk@crmes.org.br. O setor de Tecnologia da Informação irá submeter a solicitação à aprovação da Gerência para prosseguir com o atendimento.

4.4 Senhas de acesso

Somente poderão acessar a internet empregados que tenham uma chave de acesso válida do CRM-ES, uma vez que é preciso autenticar-se no servidor de *proxy* com usuário e senha de acesso.

A senha de acesso tem caráter pessoal e intransferível, cabendo ao seu titular total responsabilidade quanto seu sigilo.

A prática de compartilhamento de senhas de acesso é terminantemente proibida e o titular que fornecer sua senha a outrem responderá pelas infrações por este cometida, além

disso, estará sujeito às sanções nos Atos Normativos do Plano de Cargos, Carreira e Salários do CRM-ES aprovado pela Resolução CRM-ES n.º 338/2025.

5. Utilização do Correio Eletrônico (E-mail)

Estabelecer responsabilidades e requisitos básicos de uso dos serviços de correio eletrônico disponibilizados pelo CRM-ES, tanto no ambiente interno como no externo.

O serviço de correio eletrônico disponibilizado pelo CRM-ES deve ser utilizado somente para finalidades de interesse da autarquia.

a) O acesso a mensagens de correio eletrônico é de exclusividade do empregado detentor do endereço eletrônico, sendo garantida a inviolabilidade do conteúdo das mensagens eletrônicas, ressalvando com prévio aviso e autorização da Gerência Administrativa/Diretoria para a realização de auditorias.
b) Os empregados do CRM-ES poderão ser titulares de uma única caixa postal individual no servidor de correio eletrônico, com direitos de envio/recebimento de mensagens, via intranet e internet, enquanto perdurar o seu vínculo com o CRM-ES.
c) O envio/recebimento de mensagens, por meio de correio eletrônico, fica limitado ao tamanho máximo de 10MB (dez Megabytes).
d) É facultado ao CRM-ES estabelecer o tamanho máximo de mensagens de correio eletrônico, de acordo com a política local de uso deste serviço.
e) É vedada a utilização do correio eletrônico para veicular mensagens do tipo SPAM (e-mails não solicitados e enviados para vários destinatários).
f) O CRM-ES possui um serviço para envio de e-mails em massa. Caso necessário e com autorização da Gerência Administrativa, o serviço pode ser utilizado para divulgação de atividade relacionadas aos serviços do Conselho.
g) O usuário deve ter o máximo de certeza de que a mensagem enviada não seja considerada abusiva, obscena, ofensiva, rude ou preconceituosa.
h) É vedado o uso de e-mail para propaganda política, racial, financeira ou de qualquer outra natureza, pois fere o princípio do Conflito de Interesses;
i) É vedado o uso de material pornográfico entre os e-mails da organização, tanto recebimento como envio;
j) É vedado o uso de e-mail para difamação ou calúnia de qualquer pessoa física ou jurídica.
k) O usuário deverá verificar diariamente sua caixa de mensagens, excluindo aquelas

cujo armazenamento não mais se faça necessário;

l) O usuário deverá limitar o acesso às informações (arquivos, diretórios, mensagens, etc.) de sua responsabilidade somente às pessoas e usuários autorizados.

m) É proibido sobrecarregar o tráfego da rede do CRM-ES com grandes volumes de mensagens e/ou arquivos de áudio/vídeo;

n) É vedada a instalação e utilização, nas estações de trabalho do CRM-ES, de sistemas clientes de correio eletrônico diferentes do disponibilizado pelo setor de Tecnologia da Informação, inclusive aqueles disponíveis na internet.

o) O empregado ou terceiros prejudicados pela recepção de mensagens não solicitadas dirigidas a uma pluralidade de pessoas deverão comunicar o fato ao Setor de Tecnologia da Informação, a quem caberá efetuar diligências com o intuito de apurar os responsáveis, após comunicado e autorizado pela Gerência.

p) Não abrir anexos com as extensões .bat, .exe, src, lnk e .com, ou de quaisquer outros formatos desconhecidos ou alertados pelo setor de Tecnologia da Informação.

q) Não reenviar e-mails do tipo corrente ou com conteúdo sabidamente falsos como: aviso de infecção vírus, avisos da Microsoft, Symantec, etc., crianças desaparecidas, crianças doentes, pague menos em alguma coisa, não pague alguma coisa, etc.

r) Não utilizar o e-mail do CRM-ES para assuntos pessoais.

s) Evitar enviar anexos com tamanho superior a 5MB.

t) Utilizar o e-mail para comunicações oficiais internas, as quais não necessitem obrigatoriamente do meio físico escrito. Isto diminui custo com impressão e aumenta a agilidade na entrega e leitura do documento.

5.1 Regras para criação de e-mails e listas de discussão de e-mails

O serviço de e-mails do CRM-ES será administrado pelo setor de Tecnologia da Informação deste órgão que seguirá as normas abaixo:

a) A criação, alteração, desativação ou remoção de e-mail institucional será efetuada a partir de abertura de chamado no sistema de help desk ou via e-mail para helpdesk@crmes.org.br encaminhados pela Gerência, RH ou chefia do setor.

b) A criação de grupos de discussão, no servidor de e-mail, a inscrição, remoção de e- mails nos grupos existentes será efetuada a partir de abertura de chamado no

sistema de help desk ou via e-mail para helpdesk@crmes.org.br encaminhados pela Gerência, RH ou chefia do setor.

c) Os e-mails criados terão cota de armazenamento de tamanho fixo, de acordo com os procedimentos internos do setor de Tecnologia da Informação.
d) Os e-mails que passarem de seis (06) meses sem serem utilizados poderão ser removidos do servidor.

6. Normas para Armazenamento de Arquivos

Regras e requisitos básicos aplicadas aos ativos de informação para armazenamento de arquivos no setor de Tecnologia da Informação do CRM-ES.

a) Os arquivos da rede do CRM-ES estão disponibilizados em unidades mapeadas na própria máquina do usuário, da maneira que se segue:
    I. Diretório mapeado do setor - é uma área do disco rígido de um dos servidores, que disponibiliza para os usuários os diretórios e documentos relativos ao setor onde trabalha. É feito backup (cópia de segurança) **diário** destes arquivos, possibilitando ao usuário a recuperação dos mesmos em caso de perda acidental, desde que tenha havido tempo hábil para ao menos um backup; este diretório não deverá ser utilizado, em hipótese alguma, para gravação de arquivos particulares de qualquer tipo, arquivos de instalação ou quaisquer outros que não sejam os de trabalho.
        1. Compete ao setor de Tecnologia da Informação a realização de backup (cópia de segurança) diário do conteúdo desta pasta.
        2. Os arquivos que estiverem em desacordo com o exposto acima poderão ser apagados (excluídos) ou postos em quarentena sem prévio aviso aos usuários.
b) É proibido o uso de qualquer outra área do sistema operacional em uso nas estações de trabalho do CRM-ES para armazenamento de dados de qualquer tipo, ficando ao Setor de Tecnologia da Informação isento de responsabilidade em caso da perda de informações ali contidas;
c) Para a recuperação de diretórios ou arquivos acidentalmente excluídos, o empregado ou o chefe de setor deverá abrir um chamado junto ao setor de Tecnologia de Informação, com o máximo de detalhamento possível, para facilitar a localização e identificação do arquivo ou diretório em questão;

d) Evitar o armazenamento na rede de arquivos de instalação, imagens e arquivos sem uso. Tal procedimento sobrecarrega os discos dos servidores, tornando sua utilização mais lenta. Os backups também se tornarão maiores, mais lentos e menos eficientes devido a este fato;
e) É vedado o uso de mídias removíveis como pendrives e cartões de memória.
f) O setor de Tecnologia da Informação não fará backup de arquivos e/ou programas que estejam instalados na máquina do usuário, nem por solicitação do usuário, nem caso necessite formatar a estação de trabalho.

7. Direitos e deveres dos usuários

a) É proibido tentar ludibriar a segurança dos recursos computacionais, sistemas ou softwares;
b) É proibida a instalação de quaisquer softwares por parte do usuário, não importando o tipo de licenciamento do produto.
c) O setor de Tecnologia da Informação poderá valer-se da autonomia citada no item 2.1 deste instrumento para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).
d) É proibido utilizar sistemas ou softwares ilegais ou não autorizados;
e) É dever do usuário utilizar apenas os softwares autorizados, que forem legalmente adquiridos e instalados pelo setor de Tecnologia da Informação. É vedado o fornecimento de cópias de softwares legalmente adquiridos pelo CRM-ES para uso particular.
f) Não é permitida a cópia de softwares pertencentes ao CRM-ES.
g) É proibido conectar à rede do CRM-ES computadores ou qualquer outro tipo de dispositivo não autorizados pelo setor de Tecnologia da Informação;
h) São de responsabilidade do usuário acionamento e o desligamento dos equipamentos de informática, no início e término de cada expediente;
i) São proibidos o remanejamento e a remoção de qualquer equipamento de informática sem aviso prévio ao setor de Tecnologia da Informação;
j) É vedada a manipulação dos equipamentos de rede (switches, hubs, fiação, cabeamento de rede, entre outros) por pessoal não pertencente ao Setor de Tecnologia da Informação.
k) Não conectar ou desconectar nenhum periférico com o equipamento ligado. Tal

procedimento pode danificar tanto o periférico como o computador. Essa regra não se aplica a dispositivos *plug & play*.

l) É terminantemente proibido ao usuário o acesso ou manutenção no interior do gabinete do computador, assim como troca ou retirada de componentes do mesmo. Caso julgue necessário, o setor de Tecnologia da Informação deverá ser acionado.

m) O setor de Tecnologia da Informação não possui rotina de backup para estações de trabalho, ou seja, todo material institucional produzido e/ou alterado deverá ser gravado, necessariamente, nas unidades de rede ou em outros serviços de armazenamento fornecidos pelo CRM-ES.

n) Os serviços em equipamentos particulares não serão permitidos nas dependências do CRM-ES, exceto com a autorização do setor de Tecnologia da Informação.

o) É proibido utilizar a identidade (caixa postal eletrônica ou contas de sistemas) e senha de terceiros.

p) Não é permitido o uso de material de consumo de informática, como impressoras, para fins particulares.

q) Da mesma forma que os acessos aos sites, todo trabalho executado nas multifuncionais é registrado, inclusive com uma imagem do conteúdo do documento, a fim de compor relatórios de futuras auditorias.

8. Disposições Finais

Conforme informado, a Política de Segurança da Informação do CRM-ES concede o direito de monitorar o tráfego através das suas redes de comunicação, incluindo o acesso à internet e utilização do correio eletrônico.

A monitoração do cumprimento das normas de utilização da internet será executada, após autorização da Gerência conforme os itens abaixo:

a) O setor de Tecnologia da Informação identificará os usuários que descumprirem qualquer item desta norma de segurança.

b) Na primeira transgressão o empregado será notificado, via e-mail, sobre o item que transgrediu e orientado para não mais infringir, sob pena de sofrer outras sanções.

c) Na segunda transgressão o empregado será notificado novamente, via e-mail, mas com cópia para o Superior Hierárquico, do descumprimento das normas estabelecidas neste documento. Caso na infração cometida esteja caracterizado qualquer tipo de crime (acesso a sites de pedofilia, racismo, etc.), tomar-se-ão

providências previstas em lei.

d) Caso haja uma terceira infração da norma, o caso será avaliado pela Gerência e serão tomadas as providências cabíveis.
e) O CRM-ES se reserva no direito de verificar, sempre que julgar necessário, a obediência às normas ou procedimentos citados neste documento.
f) O uso indevido dos serviços de correio eletrônico, tratados neste documento, é passível de sanção disciplinar, de acordo com a legislação vigente e demais normas aplicadas à matéria.
g) Será de responsabilidade de cada usuário zelar pelo fiel cumprimento ao estabelecido na presente norma, devendo também assinar o "Termo Individual de Responsabilidade", anexo a esta Política de Segurança da Informação.
h) Todos os equipamentos do CRM-ES devem ser mantidos em boa condição e possuir proteção de forma a preservar seus componentes internos.
i) O usuário arcará pelos danos causados pelo mau uso dos computadores e dos recursos do CRM-ES, mediante apuração cabível, nos termos da lei.
j) A saída de equipamentos do CRM-ES deve ser feita através do documento de saída de equipamento, modelo disponível na pasta padrões do servidor de arquivo, que deverá ser autorizado pela Liderança do Setor de TI e pela Secretaria-geral do CRM-ES e entregue uma cópia ao pessoal da segurança e ao Setor de Almoxarifado e Patrimônio.
k) Computadores pessoais, bem como computadores portáteis têm que dar entrada na recepção do CRM-ES.
l) Não é permitida a manutenção técnica de equipamentos pessoais no setor de Tecnologia da Informação do CRM-ES. A equipe técnica está desautorizada a fazê-la no âmbito do CRM-ES.

9. Penalidades

O empregado que, de forma indevida ou não autorizada, apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, arquivo ou programa de computador, fizer uso indevido dos equipamentos de informática, bem como praticar ato em desacordo com os termos da presente norma fica sujeito às punições cabíveis na Consolidação das Leis Trabalhistas e também nos Atos Normativos do Plano de Cargos, Carreira e Salários do CRM-ES aprovado pela Resolução CRM-ES n.º 338/2025, desde que autorizada fundamentadamente

a abertura de procedimento administrativo disciplinar pela Presidência.

O empregado infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu líder imediato, à Gerência Administrativa/Recursos Humanos, à Diretoria correspondente e à Presidência.

Todos os empregados ao tomarem conhecimento de qualquer incidente de segurança da informação devem informar o ocorrido, imediatamente, ao setor de Tecnologia da Informação pelo e-mail informatica@crmes.org.br.

10. Membros Responsáveis

O Líder Operacional do Setor de Tecnologia da Informação ou outro empregado lotado no referido Setor, devidamente designado pela Gerência Administrativa/Diretoria, ficará diretamente responsável pela implantação e implementação da Política de Segurança da Informação no âmbito do CRM-ES. Todo empregado e/ou setor que precisar tratar de assuntos pertinentes à segurança da informação, assunto deste instrumento, deve se reportar ao responsável citado.

11. Vigência e Validade

A presente política passa a vigorar a partir da data da aprovação Resolução CRM-ES n.º 338/2025, sendo válida por tempo indeterminado.

12. Legislação

- Lei Federal nº 8159, de 08 de janeiro de 1991 (Dispõem sobre a Política Nacional de Arquivos Públicos e Privados).
- Lei Federal nº 9279, de 14 de maio de 1996 (Dispõe sobre Marcas de Patentes).
- Lei Federal nº 9610, de 19 de fevereiro de 1998 (Dispõe sobre o Direito Autoral).
- Decreto nº 3505, de 13 de junho de 2000 (Institui a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal).
- Lei Federal nº 10.406, de 10 de janeiro de 2002 (Institui o Código Civil).
- Decreto nº 7.845, de 14 de novembro de 2012 (Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento).

Obs.: Conforme a necessidade e as medidas para minimizar e combater ocorrências, outras legislações poderão ser aplicadas à matéria, conforme as legislações em vigor no país.

13. ANEXO I - Termo Individual de Responsabilidade

Eu, _____,
matrícula _____, CPF nº _____, na qualidade de usuário dos recursos de Tecnologia de Informação disponibilizados pelo CRM-ES, declaro estar ciente e concordar com a Política de Segurança da Informação do CRM-ES, que está disponível para consulta no Portal Transparência de Prestação de Contas e na intranet.

Declaro assumir toda e qualquer responsabilidade de controle, guarda e conservação dos equipamentos relacionados nesta política. Tenho ciência de que a retirada de qualquer equipamento que faça parte do parque tecnológico do CRM-ES para manutenção, assim como a instalação de qualquer software, deverá ser feita somente por empregados do setor de Tecnologia da Informação, devidamente identificados.

Declaro estar ciente de que os arquivos, documentos e e-mails que se encontram em computadores e/ou servidores de rede do CRM-ES e do CFM são de propriedade da respectiva Autarquia. Portanto, ao desligar-me do Conselho, não poderei fazer cópias de documentos, ou de softwares licenciados ao CRM-ES e CFM.

Declaro estar ciente de que devo gravar os arquivos produzidos e manipulados por mim na rede de computadores do CRM-ES e de que não existe rotina de backup para arquivos gravados localmente nas estações de trabalho.

Declaro, também, estar ciente de que os acessos por mim realizados à internet, bem como o conteúdo das mensagens enviadas através do correio eletrônico corporativo são monitorados automaticamente.

Vitória, _____ de _____ de ____.

_____
Assinatura

14. Glossário

Ativo. Tudo que tem valor para a organização.

Caixa Postal. Espaço em disco, onde são armazenadas as mensagens de correio eletrônico.

Controle. Forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

Download. Ato de copiar (baixar) um arquivo de outro computador, através da Internet.

E-mail (Eletronic mail). Correio eletrônico**,** mensagem eletrônica.

Helpdesk. Serviço de apoio a usuários para suporte e resolução de problemas técnicos.

Internet. Associação mundial de redes de computadores.

Intranet. Rede interna, de uso corporativo, que utiliza a mesma tecnologia da internet, para que os empregados possam acessar as informações dos seus respectivos órgãos.

Plug & Play. Tecnologia que permite configuração automática de dispositivos conectados ao computador. Também conhecida como PnP.

15. Histórico de Revisores

DATA	REVISOR	FUNÇÃO
25/03/2019	GUILHERME LUCIANO LEITE MARQUES	CHEFE DE T.I.
25/03/2019	VINÍCIUS MARTINS	TÉCNICO DE INFORMÁTICA
25/04/2024	WILIAN BATISTA DOS SANTOS	CHEFE DE T.I.
25/04/2024	WESLEY SILVA FONTOURA DE OLIVEIRA	TÉCNICO DE INFORMÁTICA
04/07/2024	WILIAN BATISTA DOS SANTOS	LÍDER OPERACIONAL
22/05/2025	WESLEY SILVA FONTOURA DE OLIVEIRA	LÍDER OPERACIONAL

CONSELHO REGIONAL DE MEDICINA DO EST DO ESPIRITO:31300999000118

Assinado de forma digital por CONSELHO REGIONAL DE MEDICINA DO EST DO ESPIRITO:31300999000118
Dados: 2025.07.31 14:25:14 -03'00'